

# hp SANworks

---

## Release Notes – Network View Version 2.0B SP3

Part Number: AA-RP8BH-TE

**Eighth Edition (February 2004)**

This document summarizes features and characteristics of *SANworks*™ Network View Version 2.0B SP1, SP2, and SP3 that are not covered elsewhere in the Network View documentation.

For the latest version of these Release Notes and other Network View documentation, visit the hp storage website:

<http://h18000.www1.hp.com/products/sanworks/networkview/>



i n v e n t

---

© Hewlett-Packard Company, 2004. All rights reserved.

Hewlett-Packard Company makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard. The information contained in this document is subject to change without notice.

Microsoft, MS-DOS, Windows, and Windows NT are trademarks of Microsoft Corporation in the U.S. and/or other countries.

All other product names mentioned herein may be trademarks of their respective companies.

Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein. The information is provided “as is” without warranty of any kind and is subject to change without notice. The warranties for Hewlett-Packard Company products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.

Printed in the U.S.A.

Release Notes – Network View Version 2.0B SP3  
Eighth Edition (February 2004)  
Part Number: AA-RP8BH-TE

## Release Notes Contents

- What's Changed Since 2.0B, page 4
- Hardware and Software Requirements, page 6
- Installation, page 6
- Known Issues by Category, page 11
  - General
  - Delays
  - Device Support
  - Display
  - Performance Data/ Monitoring
  - Polling Functions
  - Settings/Status
- Documentation Corrections, page 26

## Intended Audience

This document is intended for customers who purchased *SANworks*™ Network View Version 2.0B, and for HP authorized service providers responsible for installing, configuring, and maintaining systems that include Network View.

## Other Network View Documentation

The Network View documentation also includes:

- Online Help (accessible via the Web browser interface)
- SANworks by Compaq Network View Version 2.0 Installation Guide, Part Number: AA-RP8AB-TE.
- SANworks by Compaq Network View 2.0 User Guide, Part Number: AA-RS5PA-TE.
- SANworks by Compaq Network View QuickSpecs, found at the HP Web Site.

## **What's Changed Since 2.0B**

This section describes the changes to Network View 2.0B SP1, SP2, and SP3.

### **Changes in Version 2.0B SP3**

Network View v2.0B SP3 supports security for SMA software v2.1 and adds support for McData Switches with firmware versions 04.01.02 and 05.01.00.

The following list details changes that correct problems or add functions to Network View 2.0B SP3.

- Supports security for SMA software v2.1
- Supports McData firmware versions 04.01.02 and 5.01.00
- Problem with E-Ports on 2/65 core switches—Devices connected to a higher PortID than the ISL's are shown incorrectly within Network View.
- SNMP Community name cannot be changed in Network View 2.0B—SANworks Network View is not showing the SNMP devices if they have community string other than “public”
- Problems with Tru64 agents discovering HBA's—SANworks Network View is not showing HBA's if their hardware-id's are greater than 99
- Tru64 Agent installation problem fixed for 4.0f and 4.0g

### **Changes in Version 2.0B SP2**

Network View 2.0B SP2 added support for VCS 3.0 on EVA 5000.

### **Changes in Version 2.0B SP1**

The following list details a number of changes that correct problems or add functions to Network View 2.0B SP1.

- Performance memory leak—Internet Explorer used up more and more memory as additional historical graphs and live graphs were opened. Eventually the workstation performance was affected.

Internet Explorer use on client machine would grow to over 100 MB when displaying historical data multiple times. This memory space was not released until all Internet Explorer windows were closed out.

- **McData port information**—McData made a change to the MIB so only port information was available on ports with devices connected. For example, if ports 25 and 30 had active connections, they would be shown in Network View as ports 1 and 2.
- **McData performance**—Some performance metrics would overflow the space allocated and be displayed as a negative number.
- **EVA performance data**—There were errors in the calculation of response times and queue lengths as reported by Network View for EVA110 controllers and individual LUNs.
- **Registry version number showing up incorrectly in Storage Management Appliance (SMA) software v2.0**—The version number displayed by Network View help did not match the version number in the registry that the SMA reported
- **Performance capture not restarted after reboot**—Network View performance data collection stopped, if any element was enabled, after the Appliance was rebooted.
- **Help text not displaying with Netscape**—The Table of Content navigation pane of the help system was missing text for the Table of Contents, Index, and Search tabs. The Help files have been updated to properly display index on Netscape (with exception for Solaris, see Known Issues and Workarounds for explanation)
- **New function - add support for HP branded switches**—Network View was not able to recognize HP-branded switches.
- **New function- DM and Perfs services no longer require *Manual* setting**—Previously DM and Perfs services were required to be set to *Manual* (see *Storage Management Appliance software v2.0 SP1a Readme*). The Manual setting for these services is no longer required.
- **DM service stops properly when Network View services are stopped on the SMA software v2.0 SP1a**—DM service produced a timeout error when Network View services were stopped on the SMA software v2.0 SP1a (**Settings > Manage Tools**).
- **Network View no longer hangs when SMA Remote Access and Command View eva login information does not match**—If the SMA is configured to manage Enterprise Virtual Arrays (EVA) and the Command View eva (previously called the HSV Element Manager) login information set in **Remote Access** does not match the Command View eva login information, Network View hangs.
- **FixupService.exe no longer needed** (`c:\FileStore\FixupServices.exe`)—Network View 2.0B upgrade caused Network View services to no longer appear on the Manage Tools page in SMA software v2.0 SP1a.
- **Network View 2.0B SP1 configured for EVA does not hang during SMA startup**—DM service hangs when Network View 2.0B SP1 is configured for EVA controllers.
- **New function- EVA 512 LUN support**—Network View 2.0B did not discover the virtual disks when there are 512 virtual disks on the EVA subsystem.

- New function- performance logging window hanging problem in large SAN—EVA - could not obtain performance logging enabled in large SANs.

## Hardware and Software Requirements

Please refer to the QuickSpecs, found at the HP Web Site, for a detailed list of all hardware and software requirements that must be met before the Network View application can be installed on your SMA. Also, refer to the QuickSpecs for a list of the supported types of devices and the requirements that must be met before the Network View host agent can be installed on a host server. The Network View QuickSpecs along with additional documentation, including white papers and best practices documents, are available via the hp website at:

<http://h18000.www1.hp.com/products/sanworks/networkview/>

## Installation

Network View 2.0B SP3 can be installed on Storage Management Appliance (SMA) software v2.1. Network View 2.0B SP3 is in *swp* file format and is available only on the web (not on CD).

**NOTE:** If you need to run a complete new installation of Network View on SMA software v2.1, please see “Creating a New Network View 2.0B SP3 Installation on SMA Software v2.1” on page 8 for more information.

## Requirements

Before installing Network View 2.0B SP3, make sure that Network View 2.0B is installed.

Network View 2.0B SP3 is a network-installable patch that can be obtained from the following web site:

<http://h18006.www1.hp.com/products/sanworks/softwaredrivers/networkview/index.html>

## Upgrade Procedure for Network View 2.0B SP3 on SMA Software v2.1

If you have Network View 2.0, upgrade to Network View 2.0B, then install SMA software v2.1, and finally install Network View 2.0B SP3.

If you have Network View 2.0A, upgrade to Network View 2.0B, then install SMA software v2.1, and finally install Network View 2.0B SP3.

If you have Network View 2.0B, then install SMA software v2.1, and finally install Network View 2.0B SP3.

## Installing Network View 2.0B SP3 on SMA Software v2.1

Once you download the Network View 2.0B SP3 *swp* file on your computer, it is installed using one of the following two methods:

### FTP

Copy the Network View 2.0B SP3 update file to an ftp server. Install the Network View 2.0B SP3 update from SMA software v2.1 selecting a **Network Install**.

### Local Disk

1. Connect to the SMA via Terminal Services or directly attach a monitor, keyboard, and mouse.
2. Copy the Network View 2.0B SP3 update file to the `c:\Compaq\SWPInstallKits` folder on the SMA.
3. Install the Network View 2.0B SP3 update from the SMA software v2.1 by selecting **Local Disk Install**.

## Creating a New Network View 2.0B SP3 Installation on SMA Software v2.1

Follow this procedure to install Network View 2.0B SP3 on an SMA that is already running SMA software v2.1. Use these procedures after restoring an appliance to SMA software v2.1 using a QuickRestore CD.

There are three steps you must follow to create a new installation of Network View 2.0B SP3 on SMA software v2.1.

- Install Network View 2.0
- Install Network View 2.0B
- Install Network View 2.0B SP3

### Installing Network View 2.0 on SMA Software v2.1

1. Connect to the SMA either using Terminal Services or by connecting a monitor, keyboard, and mouse directly to the SMA.
2. Insert the *NetworkView\_V20* CD-ROM in the CD/DVD-ROM Drive on the SMA.
3. Execute the following commands in a Command Prompt window:

```
Cd\  
D:  
cd Network_View  
setup.exe
```

**NOTE:** If the CD/DVD-ROM drive letter is not D, substitute the correct drive letter for the above command.

4. Proceed with the interactive installation of Network View. When the installation is complete, execute the following commands in the Command Prompt window:

```
C:  
cd c:\mysql\bin  
mysqld --remove
```

5. Restart the SMA.
6. When the SMA is restarted, stop the Network View services by running the following batch file:

```
C:\Program Files\Compaq\SANworks\Network  
View\HMMO\server_batch_files\StopNVServices.bat
```



7. Execute the following commands in the Command Prompt window:

```
cd\  
cd c:\mysql\bin  
mysqld -install  
net start mysql
```

The Network View 2.0 installation is complete.

## Installing Network View 2.0B on SMA Software v2.1

1. Ensure that Network View services are stopped, even if you are continuing the installation for the previous section. If necessary, run the following batch file on the SMA to stop the Network View services:

```
C:\Program Files\Compaq\SANworks\Network  
View\HMMO\server_batch_files\StopNVServices.bat
```

2. Download and install the Network View 2.0B patch. You can download the *swp* file from the following website:  
<http://h18006.www1.hp.com/products/sanworks/softwaredrivers/networkview/>
3. Once you download the Network View 2.0B *swp* file on your computer, it can be installed using one of the following two methods:

### FTP

Copy the Network View 2.0B update file to an ftp server. Install the Network View 2.0B update from SMA software v2.1 selecting a **Network Install**.

### Local Disk

- a. Connect to the SMA either using Terminal Services or by attaching a monitor, keyboard, and mouse directly to the SMA.
- b. Copy the Network View 2.0B update file to the  
c:\Compaq\SWPInstallKits folder on the SMA.
- c. Install the Network View 2.0B update from the SMA software v2.1 by selecting **Local Disk Install**

## Installing Network View 2.0B SP3 on SMA v2.1

1. Download and install the Network View 2.0B SP3 *swp* file. You can download the *swp* file from the following website:  
<http://h18006.www1.hp.com/products/sanworks/softwaredrivers/networkview/>
2. Once you have download the Network View 2.0B SP3 *swp* file on your computer, it is installed using one of the following two methods:

### FTP

Copy the Network View 2.0B SP3 file to an ftp server. Install Network View 2.0B SP3 from SMA software v2.1 selecting a **Network Install**.

### Local Disk

- a. Connect to the SMA either using Terminal Services or by attaching a monitor, keyboard, and mouse directly to the SMA.
- b. Copy the Network View 2.0B SP3 file to the `c:\Compaq\SWPInstallKits` folder on the SMA.
- c. Install Network View 2.0B SP3 from the SMA software v2.1 by selecting **Local Disk Install**.

## Known Issues by Category

The topics are:

- General, page 11
- Delays, page 14
- Device Support, page 14
- Display, page 18
- Performance Data/ Monitoring, page 20
- Polling Functions, page 22
- Settings/Status, page 23

## General

### Dropping the Network View Database Tables

Network View does not provide a way to remove devices from the topology map unless the devices are in a Critical status. The procedure described below can be used to remove all devices and associated events from the device database and (optionally) all performance information from the performance database. It should be noted that when Network View is started, the device database is populated with SNMP devices found within the IP address discovery ranges as well as systems running a Network View host agent which report to the SMA.

### Preparing to Clear the Databases

1. Launch the *SANworks* Network View application.
2. Modify the IP Address Ranges for Discovery as necessary in the Application Configuration window.
3. Connect to the SMA using Terminal Services or by attaching a monitor, keyboard, and mouse.
4. Stop all Network View services by executing the following batch command:  

```
c:\Program Files\Compaq\SANworks\Network View\HMMO\server_batch_files\
StopNVServices.bat
```

## Clearing the Databases

1. Insert the *SANworks* Network View 2.0 product distribution CD into the CDROM drive on the SMA. Open the \MySQL\_gui folder and double-click on mysqlgui.exe to run the MySQL GUI client.
2. Click OK at the password prompt (no password). On the left hand side of the MySQL GUI Client below the menu bar, the 'Connected' icon should be green and the database you are connected to should be NETWORKVIEW.
3. In the top pane of the MySQL GUI Client, enter the command 'drop table element' and click the Execute Query. When the cursor returns to the beginning of the line, type 'drop table eventlog' over the previous command and click Execute Query. After the commands are executed, they are copied to the bottom pane in the window.
4. (OPTIONAL) To drop the tables in the performance database, select the PM database from the drop down box that currently shows NETWORKVIEW. Using step 3. as an example, execute the following commands in the top pane of the MySQL GUI client window:
  - drop table pmstats
  - drop table pmdevices
  - drop table pmprop
  - drop table pmstrmap
  - drop table pmthresholds
5. Close the MySQL GUI client window

## After Clearing the Databases

1. Start the Network View services by executing the following batch command:  
c:\Program Files\Compaq\SANworks\Network View\HMMO\server\_batch\_files\  
StartNVServices.bat.

## **Firewall Support**

The SMA on which the Network View server operates must be collocated with supported Host Agents inside a firewall. Communication between the SMA and Host Agents through a firewall is not supported. Opening various ports required to enable Host Agent communication may compromise the security of your network and is not recommended.

## **Network View Host Agent for Novell Netware**

The Network View Host Agent for Novell Netware is automatically installed on the SMA. There are no agent installation steps required for a Netware system. However, the IP addresses for the Netware systems must be in the Network View discovery range. The SANworks Network View QuickSpecs, found at the HP Web Site, lists the minimum software and hardware requirements necessary to run Network View with Novell NetWare.

## **Cannot Uninstall Network View Using SMA Software Interface**

You cannot uninstall Network View using the SMA software interface.

## **Renaming the Storage Management Appliance**

If you want to rename the SMA, it must be done prior to installing Network View since the name is internally stored by Network View. This is the expected behavior.

## **Delays**

### **Status of Failed Devices Takes a Long Time to Display**

Devices or hosts that fail to respond to Network View status polls may not show a status change for up to an hour. This is the result of an increase of the heartbeat interval from 15 to 30 minutes which was done to support the Enterprise Virtual Array.

### **Web Server Login Page Time-out**

If you are logged in to Network View and leave your page open with no activity for longer than the time-out period set by the Web Server, you will lose connectivity to some of the functions in Network View. If you refresh your screen, the Login window appears again and you can login using your previous login.

## **Device Support**

### **Deleting Devices from the Network View Map**

To delete a SNMP device from the topology map, ensure its IP address has been removed or excluded from the IP address discovery range in the Application Configuration window and then shutdown the device. After about 15 minutes, Network View will detect that the device is in a Critical status. Right-click on the device icon and choose Delete to delete the device from the map. To delete a host agent from the map, stop the Network View service, process, or daemon on the host system, wait for the host to appear Critical on the map, and then delete the host. To delete all hosts and devices from the topology map, see release note, Dropping the Network View Database Tables in this document.

### **Devices Automatically Added to the Discovery Range**

If a device sends a SNMP trap to the SMA, that device is automatically added to the IP Address Discovery Range. Use the Hide Device function to prevent any unwanted device from being displayed or monitored.

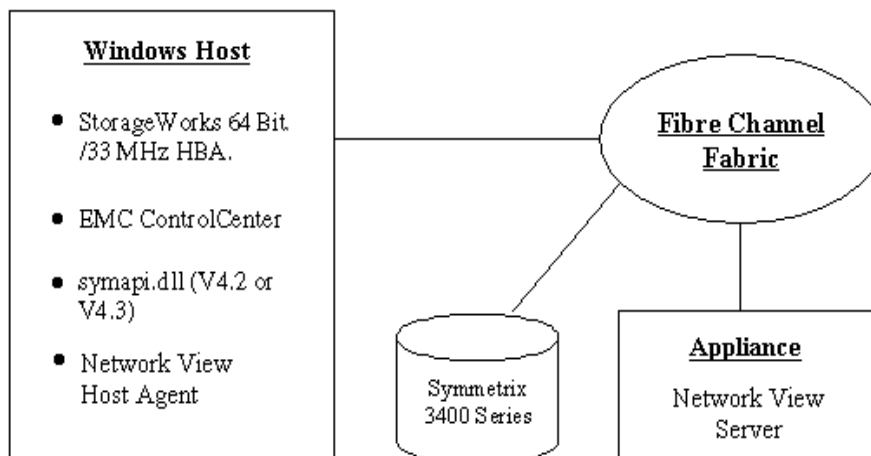
## EMC Device Support With Network View

Referring to Figure 1, Network View provides support for EMC ControlCenter running on a server with a *StorageWorks* 64Bit/33MHz HBA. In order for Network View to be able to discover and monitor the EMC Symmetrix subsystem and launch the EMC management application (EMC ControlCenter client), you need to perform the following steps:

1. Prior to installing and configuring Network View, ensure the EMC Symmetrix is properly configured. Ensure the EMC ControlCenter software has been installed on a Windows 2000 or Windows NT host. Ensure the EMC Symmetrix and the Windows host system are connected to the fabric and Network View has been configured to discover the fabric switch or switches.
2. Install the Network View Windows Host Agent on the Windows 2000 or Windows NT host system. Ensure the host system is connected to a SAN switch in the fabric.
3. On the Windows 2000 or Windows NT host system, copy the symapi.dll from c:\program files\EMC\symcli\ddl to c:\program files\compaq\sanworks\network view agent\hmmo\bin
4. On the Windows 2000 or Windows NT host system, edit devicemgr.properties in c:\program files\compaq\sanworks\network view agent\hmmo\config\nm to include the line com.prisa.nm.devicemgr.scsi.Symmetrix  
**NOTE:** This line is commented out.
5. Restart the Network View-DM service on the Windows 2000 or Windows NT host system.
6. Browse to Network View and locate the EMC Symmetrix subsystem in the topology map. Right-click on the subsystem icon, choose Properties from the popup menu and enter the following URL in the Device Management URL field: <http://hostname:40727/setup.html> substituting hostname with the name of the Windows host where the EMC ControlCenter software is installed.

7. To manage the EMC Symmetrix subsystem from Network View, double-click on the subsystem icon in the topology map. The first time you do this, you will be prompted to download and install the EMC ControlCenter client software onto your browsing machine. Follow the prompts to install the client software.

**Figure 1: EMC Configuration**



## Names of Renamed Devices May Not be Consistent Between Network View and Device Management Applications

If you rename a device or create an alias for it in its management application (if supported), the new name or alias will be used in Network View. However, if you rename a device in Network View, the name will no longer match the name used in the device's management application. To have Network View use the name or alias from the device's management application, clear the Name field in the device's Property window.



## Enterprise Virtual Array Requires Configuration of Remote Access

Network View support for the Enterprise Virtual Array requires the Remote Access feature for SMA software to be configured to setup the CV EVA password.

You can launch the Remote Access by choosing **Settings > Remote Access**.

### Configuring Remote Access

The CV EVA application is already added for your convenience but you need to enter your username and password to make it complete. Select the CV EVA application and select **Properties**, enter the username and password that will be used to access the specific CV EVA. (Refer to the *HP StorageWorks Command View EVA Getting Started Guide* for more information.)

If you accidentally Delete the CV EVA application, create a New application and select CV EVA as the application in the drop-down menu, and enter the username and password that will be used to access the specific CV EVA. (Refer to the *HP StorageWorks Command View EVA Getting Started Guide* for more information.)

## Discovery of the McData ED5000 Switch

The ED-5000 is automatically displayed, after the SDCM laptop server is discovered.

To discover the SDCM laptop server, you must enable the SNMP agent on the laptop, then discover the laptop IP address itself. Network View uses SNMP to discover these devices.

Once the laptop is visible in the topology map, you can either double click or right click the icon to launch the managed device URL. This will prompt you to either install the SDCM client or launch the SDCM client on the host browser PC. If the SDCM client is already installed, you can select the launch option, thus launching the SDCM server for managing the McData switches.

## Display

### Displaying the IBM Enterprise Storage Server

If an IBM Enterprise Storage Server is connected to a discovered switch, it appears in the map view as an Unknown System. Although Network View cannot monitor this device, you can open the Properties page for the Unknown System icon, change its device type to Storage System and add the appropriate URL to the Device Management URL field. The device now appears as a storage system and a double-click on the icon launches the IBM management application.

### Hidden Devices are Not Displayed With Unhide Device After an Appliance Reboot

If you attempt to show a hidden device on the topology map using the Unhide Device function after the appliance has been rebooted, the device will appear in the navigation pane (tree view list) but not in the map. Refresh or restart the browser to display the device in the topology map.

### HSG Controller Disappears from Tree View

If a controller fails in an HSG subsystem configured for transparent failover mode, it will no longer appear in the tree view. When the controller comes online again, refresh the browser window to view the controller. Refreshing the browser may take several minutes to correctly show the active ports on the controller because the subsystem needs to reconfigure the controller.

### Hub and Router Device Management Page May Not Display Data

The device manager pages for hubs and routers may not display device data correctly. The workaround is to reboot the appliance.

### Network View Displays an Unintelligible Name for a Hub

Setting the Sysname value should be a part of configuring your hub to ensure that Network View displays the proper name.

### Windows Host System With a StorageWorks 64-Bit/66-MHz HBA May Not Display Status Change

The Windows host system may not display a status change unless the *StorageWorks* 64-bit/66-MHz HBA also has a status change. This is current expected behavior.

## Help Display Problems with Netscape on Solaris

The SMA software HTML-based help system does not display as expected with Netscape on Solaris. The navigation pane (Contents, Index, and Search) does not display. Use one of the following methods to work around the problem:

- Use the context-sensitive help (question mark) available on each page. Clicking the question mark does display the help topic for the current page and you can follow links within these topics. Many of the context-sensitive help pages have a Related Topics button, which you can also use to navigate the help system.
- If you want to use the navigation pane, change the file name to toclist.htm at the end of the URL in the help window's Address box. For example: <http://12.20.22.100/help/0409/toclist.htm>. This displays the Contents and Index tabs without the content pane. You can click the hyperlinks to navigate the entire help system.

## Caching of JAR files not supported with Netscape 6.2.3

Caching of JAR files in Network View 2.0B SP2 is not supported for Netscape 6.2.3 on Solaris and JRE 1.4. This is a known problem when using a Netscape web browser on a Solaris machine.

## Clearing the Java Console On Tru64 and Sun Solaris Systems

When using one host computer to browse to multiple appliances, the java cache may contain data based only on one of the appliances. This may result in an error message RMI “access denied”. To clear this condition, the Java cache must be cleared.

To clear the java cache on both Tru64 and Sun Solaris systems, complete the following steps:

1. Close all browser windows.
2. Open a console window and change directory to /usr/opt/java131/bin (directory path will vary depending on the installation path).

**NOTE:** If you are not sure where the executable is stored, execute the following command:

```
# find / -name ControlPanel -print
```

The executable is located in a bin directory within the plugin directory path structure you are using.

3. Execute the following command: `# ./ControlPanel &`

4. The ControlPanel will load, click the cache tab.
5. Click the Clear JAR Cache button.

## **Incorrect Java Plug-In Might Be Downloaded**

Network View requires the browser to be configured with the Java 2 Runtime Environment, Standard Edition 1.4.1\_03 plug-in for Windows. If this plug-in is not installed, you will be prompted to download and install a plug-in from the Sun Microsystems web site. However, the plug-in that is downloaded by default might be a version that is incompatible with your browser or browser platform. You should download the correct Java plug-in v1.4.1\_03 and configure your browser before running Network View.

## **Performance Data/ Monitoring**

### **Network View is Unable to Extract Performance Data From Managed Storage Arrays**

From time to time, due to transient conditions on the management appliance, Network View is unable to extract performance data from managed storage arrays. Individual data points may be lost as a result.

When performance data is graphed for the device in question, the missing data points are not represented. The line of the graph is drawn directly between the last good data point before the missing statistics and the first good data point immediately after the missing statistics. No visual indication is given that intervening data points do not necessarily exist.

To determine if a particular range on the graph represents known data points, bring up the table of collected information for the device and examine the data manually.

### **No Performance Functions on Enterprise Virtual Array Controller Ports**

Performance data for controllers is monitored in Network View, but the data is not accessible at the port level. Performance data monitoring on Enterprise Virtual Array controller ports is not performed even though the Performance menu is enabled. If you right-click on a controller port in the tree view and select the Performance menu item, the Performance options appear, but, none of the options work. However, you can get this information by monitoring the corresponding switch ports.

## **Performance Monitoring of Virtual Disks in Enterprise Virtual Array**

Performance monitoring of virtual disks on the Enterprise Virtual Array is only enabled for those virtual disks which are presented to a host.

## **Additional Performance Statistics for McData ED5000 and SAN Director 64 Switches**

If the topology map displays both hp and McData switches, the performance statistics listed for the hp switches include additional statistics which are only appropriate for the McData switches.

When monitoring performance for the hp switches, switch ports, links, and loops, ensure only the following statistics are used:

Bytes tx; Bytes rx; Bytes thru; Bytes high; Frames tx; Frames rx; Frames thru; Frames high

## **Performance Monitoring Not Available on MSA1000 Switch Links**

Performance monitoring is not available on links between the Modular Storage Array 1000 switch and other devices/hosts. If you right-click on a link, the Performance menu item is displayed even though performance monitoring is not supported.

## **Performance Thresholds For 2 GB Switches**

The performance threshold settings for statistics on the SAN Switch2/16 are based on maximum values calculated for a 1GB 16 port switch. Modify the max value in the Threshold Configuration window for each SAN Switch2/16 statistic.

## **No Performance Functions on Controller Ports**

Performance data for controllers is monitored in Network View, but the data is not accessible at the port level. Performance data monitoring on HSG60/HSG80 controller ports is not performed even though the Performance menu is enabled. If you right-click on a controller port in the tree view and select the Performance menu item, the Performance options appear even though none of the options work. This is expected behavior.

## **Polling Functions**

### **Devices With Long Performance Polling Intervals**

When viewing a Live Graph of performance statistics collected from a device with a long performance polling interval, an adjustment is necessary. Adjust the “Time Scale” parameter of the graph display to ensure that enough data falls within the window at any given time to make a meaningful display. To change this setting, right-click on the graph, and select the appropriate item in the pop-up menu.

### **No Polling Function on Enterprise Virtual Array and HSG Logical Virtual Disks**

If you right-click on a logical virtual disk in the tree view and select Properties, the Polling Rate option appears in the page even though this option will not function. There is currently no workaround.

### **Enterprise Virtual Array Locks Out Network View Polling**

When the Enterprise Virtual Array Element Manager is performing operations on the storage subsystem, Network View’s polling is locked out. The status of the Enterprise Virtual Array is displayed as Unknown while the controllers and ports are displayed as Critical. During this time Network View and CV EVA may display a different status. The next successful Network View polling returns the correct Enterprise Virtual Array status.

### **Minimum Polling Rate for Enterprise Virtual Array Discovery**

The default status polling interval for Enterprise Virtual Array subsystems, controllers, and logical units is set to 30 minutes. Keep the minimum polling rate for Enterprise Virtual Array discovery, under all circumstances, equal to or higher than 15 minutes. If not, the Enterprise Virtual Array Element Manager becomes locked by Network View requests and is unable to serve information to any other application. If the status polling interval for a Enterprise Virtual Array is set below 15 minutes, which is against the minimum recommended interval, it will be reset to 15 minutes.

### **Enterprise Virtual Array Controller Performance Polling Interval**

The default performance polling interval for Enterprise Virtual Array subsystems, controllers, and logical units is set to 15 minutes. As with other performance-enabled devices in the SAN, the user is able to adjust the polling interval for the Enterprise Virtual Array components.

Due to architectural limitations of the hardware, the polling interval for these devices should not be set to a value greater than 30 minutes. If the polling interval is set to a value greater than 30 minutes, Network View cannot guarantee the availability of performance metrics.

Likewise, care should be taken to avoid setting the performance polling interval to a value too short. Every call to the Enterprise Virtual Array Management server risks blocking other applications from accessing the device. If the polling interval is set too short, it is possible that Network View will disrupt other applications which are trying to manage the hardware. In any event, the polling interval should never be set to less than 10 seconds.

**NOTE:** If you have a large Storage Area Network environment, it is possible that a situation can develop where performance data reporting can not take place on the Enterprise Virtual Arrays. This may be caused by Network View 2.0B status polling, combined with the status polling being done by the Enterprise Virtual Array's management interface, and any other work being done by other applications such as EVM 2.0D, DRM or SAN Scripter.

## HSG Controller Performance Polling Interval

The default polling interval for HSG80/HSG60 subsystems, controllers, and logical units is 3 minutes. For optimum performance, do not set the performance polling interval in the Live Graph or Logging Configuration window below 3 minutes.

## Settings/Status

### Appliance Removal From IP Network

If the appliance is disconnected from the IP network for more than 30 minutes, polling and discovery services may stop. All switches, routers, hubs, and storage subsystems display a critical status.

To remedy this condition, you must reconnect the SMA to the network and restart all Network View services using **Manage Tools** from the SMA software (**Setting > Manage Tools**).

### Heartbeat Missing Event in Event Log has Severity “None”

If you have upgraded from earlier versions of Network View, the severity of Heartbeat Events is not the same as it was in earlier versions. Heartbeat Events were previously set at “Critical”, they are now set to “None”.

## **Appliance Displays Warning Status on Initial Launch**

At the first launch of Network View 2.0B, the appliance will report a status of Warning if *SANworks* Password Manager is not installed. This Warning status will change to an OK status after about fifteen minutes. The appliance's events dialog then logs the following error “Password Manager not installed on appliance X”. X is the name of the appliance.

## **Uninitialized Storage Subsystems Are Not Discovered By Network View**

Any uninitialized storage subsystems are not discovered by Network View. Ensure you have not used the name “Unknown Storage System”, when installing storage subsystems. This name is ignored during the Network View discovery process.

## **Unable to Update Status of Logical Virtual Disks**

Network View is unable to display an updated status of logical virtual disks. There is currently no workaround.

## **Multiple Enterprise Virtual Array Icons After Re-initialization**

If you re-initialize an Enterprise Virtual Array that is already displayed in your Network View topology map, a second set of Enterprise Virtual Array icons may be displayed.

To correct this condition do the following:

- Wait for the old Enterprise Virtual Array icon to go into a Critical status. This can take over an hour and is the result of missing the heartbeat.
- Delete the icon in the Critical status. Once the old icon is deleted, during the next discovery cycle all LUNs and controllers move to the correct Enterprise Virtual Array.

## **Arbitrated Loop Switch 8 (FC-AL) Has the Wrong Device Management URL**

The URL for the device management application in the Arbitrated Loop Switch 8 is incorrect. Right-click on the switch icon, select Properties and change the Device Management URL to `http://switch-name` where switch-name is the name of the Arbitrated Loop Switch.



## **Cannot Use Host Name in a SNMP Trap Notification**

Host names cannot be entered in the field for SNMP trap destinations in the Notifications window. Only IP addresses can be entered in the field. The correct port information must follow the IP address as well. XE 2.1 uses port 162.

## **HSG Controller Properties are Incorrect After Controller Is Reconfigured**

If an HSG subsystem reconfigures its ports, due to a controller failure or controller coming online, the Property window for the controller may show incorrect port information. Refresh the browser window to show the correct port information for the controller.

## **Raid Array 4100 Shows Status as OK, One Controller Shows Status as Critical**

This note is for a RAID Array 4100 that is configured with redundant controllers. If one of the controllers fails, Network View reports the RAID Array 4100 unit status as degraded in the Warning status, and reports the controller status as failed in the Critical status. After a few minutes, the RAID Array 4100 unit status changes to OK, while the controller status remains Critical. This behavior is currently a function of the RAID Array 4100 and is reflected by Network View. The Raid Array 4100 does not remember that it once had a functioning controller, after the initial status change. There is currently no workaround.

## **Viewing Network View Traps in CIM-XE**

The severity level of traps displayed in Insight Manager (CIM) XE from Network View doesn't match the actual severity level of the Network View traps. You can edit the revision file in CIM XE to change severity level of the traps.

In order for traps from Network View to appear in CIM XE, do the following:

- Add the TPC/IP address of the management appliance to the TCP/IP discovery range in CIM XE and run the discovery process.

This action registers the appliance in the CIM XE and permits trap forwarding from Network View to CIM XE.

## Documentation Corrections

### Changes to Chapter 9 in the Network View User Guide

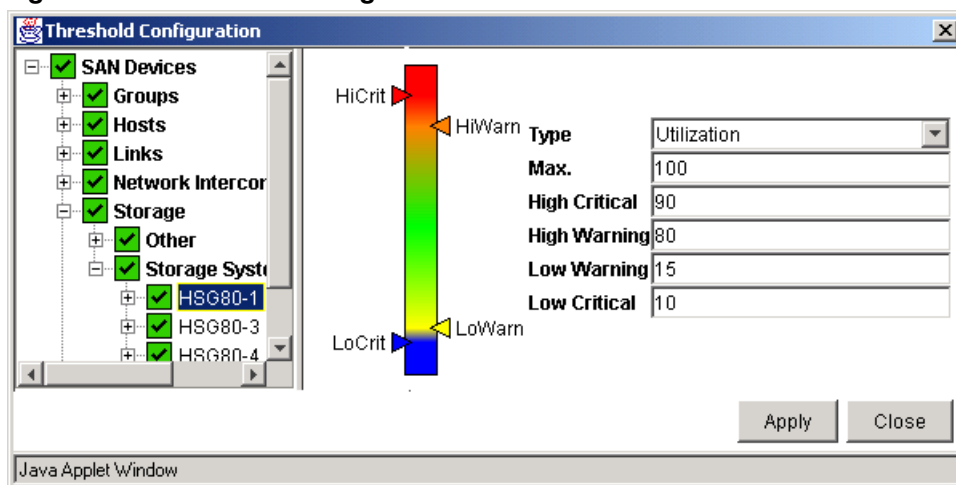
This section contains corrections to Chapter 9 in the SANworks Network View 2.0 User Guide, Part Number: AA-RS5PA-TE. These changes were not included in the released version.

#### Threshold Configuration

The Threshold Configuration window is used to set the upper and lower performance statistic thresholds for connections, subsystems, controllers, logical units, and switch ports. A threshold is used as a triggering point for an event.

Link and loop thresholds are viewable on the topology map and change color according to the Threshold Configuration selection. When devices are configured for polling or logging, the threshold range appears on the graphs.

**Figure 9-2: Threshold Configuration**



The Threshold Configuration window displays the device tree on the left. Select a device from the tree for which you wish to set threshold levels. When a device is selected, the list of statistics Network View generates for that device appears in the drop-down menu on the right. The list of statistics varies, depending on the type of device selected. For a complete list of threshold types and a description of each, see SANworks Network View 2.0 User Guide (part number: AA-RS5PA-TE) Appendix B.

Each statistic generated from a type of device is provided with a maximum value. This number represents the highest theoretical value the statistic is capable of reaching, given an ideal hardware configuration and workload for that particular statistic.

**NOTE:** No one hardware configuration will be able to maximize all statistics available from a given device.

When setting threshold levels, you are advised to examine the logged performance data for the device and select reasonable thresholds based on past history.

You can enter the following threshold levels for each type:

- High Crit
- High Warn
- Low Warn
- Low Crit

**NOTE:** This numeric value must be less than the Max. value, typically a percentage of the maximum value in numeric form. For example, if 100000 is the Max. value, then  $100000 \times 90\% = 90000$ ; enter 90000 into High Crit.

Alternately you can adjust the threshold settings by selecting one of the threshold arrows and dragging it up or down to the level you want to set.

When a device reaches one of these levels, the system generates an event.

## Changes to Appendix B in the Network View Installation Guide

This section contains corrections to Appendix B, Network View Host Agent for Tru64 Unix in the SANworks Network View Version 2.0 Installation Guide, Part Number: AA-RP8AB-TE. These changes were not included in the released version.

### Installing the Agent

**IMPORTANT:** Before you install the Network View Host Agent, complete the steps found in "Before Installing the Agent" of this appendix.

1. At the command prompt, type the following:

```
# setld -l /mnt/HOSTAGENTS/Tru64/SNV100
```

## Changes to Appendix C in the Network View Installation Guide

This section contains corrections to Appendix C, Network View Host Agent for Sun Solaris, in the SANworks Network View Version 2.0 Installation Guide, Part Number: AA-RP8AB-TE. These changes were not included in the released version.

### Installing the Agent

**IMPORTANT:** Before you install the Network View Host Agent, complete the steps found in “Before Installing the Agent” of this appendix.

1. At the command prompt, type the following:

```
# pkgadd -d /cdrom/networkview_20a/HOSTAGENTS/Solaris CPQsnview
```

## Changes to Appendix E in the Network View Installation Guide

This section contains corrections to Appendix E, Network View Host Agent for IBM-AIX, in the SANworks Network View Version 2.0 Installation Guide, Part Number: AA-RP8AB-TE. These changes were not included in the released version.

### Installing the Agent

There are multiple ways to install Network View Host Agent from IBM-AIX. The following is recommended.

### Using the Command Prompt

To install the Network View Host Agent, at the command prompt, type the following:

1. To create a mount point (directory), Example: cdrom  

```
#mkdir cdrom
```
2. To mount the CD on the created mount point:  

```
#mount -v cdrfs -o ro /dev/cdo /cdrom
```
3. To change the directory where the host agent is located:  

```
# cd /cdrom/HOSTAGENT/aix
```
4. Install the agent:  

```
# installp -Xacd cpqsnview.bff all
```

## Changes to Appendix F in the Network View Installation Guide

This section contains corrections to Appendix F, Network View Host Agent for HP-UX, in the SANworks Network View Version 2.0 Installation Guide, Part Number: AA-RP8AB-TE. These changes were not included in the released version.

### If vold is Running

1. Insert the CD-ROM into the drive.
2. Use the mount command to verify that the volume manager has automatically mounted the CD-ROM by typing the following:

```
# mount
```

**NOTE:** The system may take a few seconds to mount the CD-ROM. If the mount command does not indicate that the CD-ROM has been mounted, wait a short interval and then repeat the command. You may need to use the volcheck command to force vold to check for mounted media.

3. Press **Return**.
4. Change to the Network View directory by typing the following:

```
# cd /cdrom/networkview_20a/hostagents/hp-ux
```

5. Press **Return**.